International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 11 • Issue 1 pp. 766-769 Jan 2019-June 2019 www.csjournals.com

Enhanced Security Implementation to Prevent Cyber Crime Using Cryptography

[1]Lajja, [2]Priyanka
[1]Research Scholar, [2]Asst. Professor
Deptt. Of computer science and application, Chaudhary Ranbir Singh University, Jind, Haryana, India

Abstract: In this paper has explained the cyber crime and its effect. The crimes, that takes place with the use of the Internet. These types of offences are referred as Cyber Crime. The Network security controls have been applied to stop the entry of hackers in networks. For this purpose the firewall, virtual private networks and encryption algorithms are used. In this method of security, the virtual private network has an essential to stop the crackers from entering in networks. VPN offers the end users a way to personally get the information on the network. It may be on a public network system as internet. Cryptography with Steganography is used to stop the cyber crime. This paper would be useful for those who do not have the knowledge of cyber crime and its effect. It would be helpful to identify the trends of crime in cyber sector. To know the effectiveness of law regarding cyber crime is also determined here.
Keyword: Cyber crime, Steganography, Cryptography, Phishing, Cyber Terrorism, Spamming, Hacking, fraud, Visual cryptography, Encryption, Decryption, upload, download.

[1]INTRODUCTION

In cyber crime the digital technologies are used to commit the crime. These illegal activities includes the activities like attacking on Data System, theft of goods online etc. the child pornography, create graphics, online fraud dealing. There are also deployments in internet illegal activities. Illegal activities may be virus, worm, and any third person mistreatment as phishing and email scams etc. In this method of security, the virtual private network has an essential to stop the crackers from entering in networks. VPN offers the end users a way to personally get the information on the network. There is a growing threat of attacks on computer systems via telecommunication networks, theft or telecommunication services and the user of computer to commit fraud and crimes of data manipulation.

[2] OBJECTIVES

There are several objectives that are put forward in the research work. Such objectives are listed below:

- To identify the problems and challenges in cyber sector due to crime.
- To identify the trends of crime in cyber sector.
- Highlight present state of response to cyber offence in India;
- Highlight the level of main concern cyber crime for law enforcement association.
- To know the effectiveness of law regarding cyber crime.
- Set the recommendations for additional knowledge and feasible enhancement in state of give the answer to cyber crime in India.

[3]PROBLEM STATEMENT

Present issues &technical challenges for investigation and prevention of cyber crime in India.
There are different type of hacker and crackers who are responsible for cyber crime. A black hat may be any person who is capable to access the computer system. He accesses the system having not authority to the owner of system. Especially it has been done by malicious intention. These activities may be legal or illegal according to the laws of a country. Generally is called software cracking. A Grey Hat is skilled hacker. Sometimes he plays his role legally. But in few situations he also acts illegally. A Grey Hat hacker is the amalgam of white with black hat hacker. Usually they don't attack for personal achievement. The Internet crime hackers perform the crime on the platform of internet. It also involves the kidnapping children, scams, cyber terrorism also commit by the internet. These offences are committed by computer.

[4] IMPLEMENTATION WORK

In this research, a server application and client application have been developed by us. These applications have been created in Net bean IDE. These are indicated by the below given figure:

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 11 • Issue 1 pp. 766-769 Jan 2019-June 2019 www.csjournals.com

(a)Server Side Implementation

In this research, a server application and client application have been developed by us. These applications have been created in
Net bean IDE. These are indicated by the below given figure:

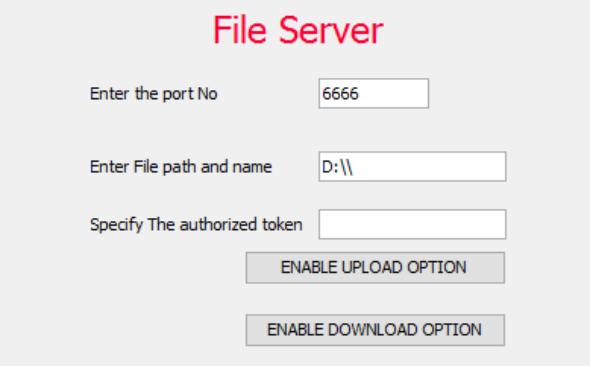

Fig: 1 The Design View of Server Side Application

(b)Client side implementation

The below given is the design view for file client in to upload and download the information. Port no, file path are specified here. Here the IP address of server and token (to encode data) are also specified.

Fig: 2 Code to implement UPLOAD on client side

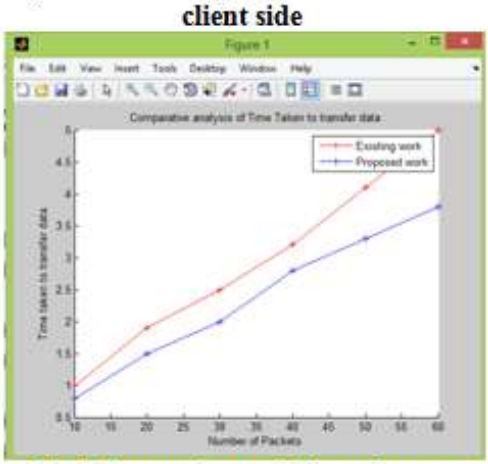

Fig 3 Comparison of time taken to transfer packet

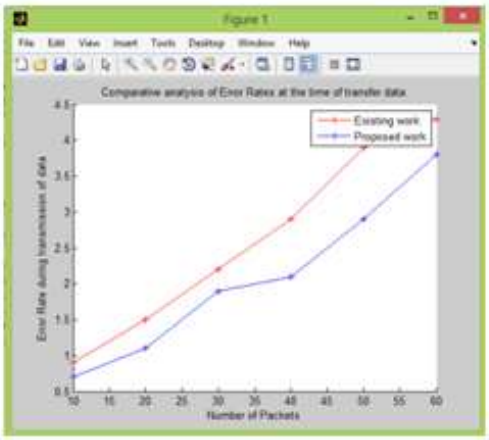

Fig 4 Comparison of error rates at the time of transfer data

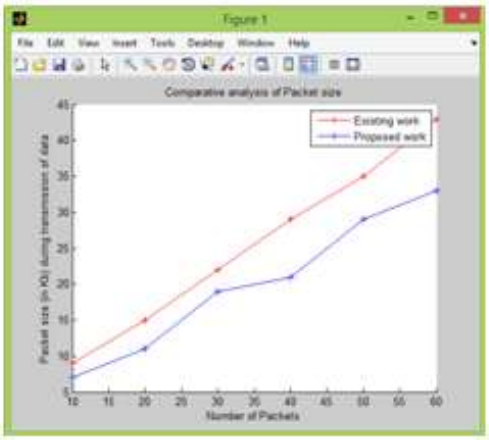

Fig 5 Comparison of packet size

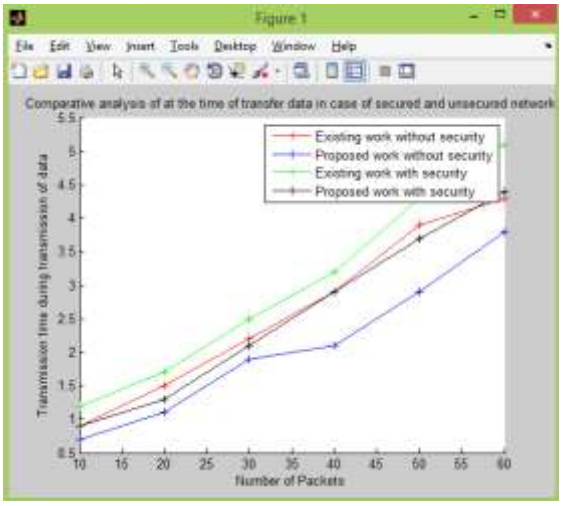

Fig 6 Comparative analysis of transmission time taking by traditional and proposed work

[5]CONCLUSION

To identify the trusted data sources and marking data get from trusted, the dynamic tainting has been used. We can give the example of SQL keywords and operators. By this method, we reduce issue of false negatives resulted from not complete clarification of all untrussed sources of data. False positives are feasible in special conditions. The traditional testing sharing delay in packet transmission and. The research work also considered the Testing processing delay at the time of packet sharing. We also make study of testing queuing delay of network packets in cloud environment. Dual Steganography has been used to resolve the security challenges. Dual Steganography has been known as the mixture of Cryptography and Steganography.

[6]FUTURE SCOPE

The research objective is the avoidance of cyber crime with the use of cyber laws as well as cyber security techniques. The cyber security techniques categorizes correctly and sufficiently. These are capable to detect the doubtful URLS. These capture the malware samples. The phishing websites are also captured with the use of clustering mechanisms. Nowadays the security tests are efficient to capture the web application susceptibilities with the use of balanced concept.

References

[1] Abhishek Kumar Bharti, ”Detection of Session Hijacking and IP Spoofing Using Sensor Nodes and Cryptography”IOSR Journal of Computer Engineering (IOSR-JCE)e-ISSN: 2278-0661, p-ISSN: 2278-8727 volume 13, Issue 2 (Jul. -Aug. 2013), PP 66-73

[2].Hani Alshamrani, “Internet Protocol Security (IPSec) Mechanisms”, International Journal of Scientific & Engineering Research, Volume 5, Issue 5, May-2014, pp. 85-87.

[3].ChanderDiwakar, Sandeep Kumar, Amit Chaudhary, “SECURITY THREATS IN PEER TO PEER NETWORKS”, Journal of Global Research in Computer Science, Volume 2, No. 4, April 2011, pp. 81-84.

[4]. HaroonShakiratOluwatosin, “Client-Server Model”, Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 1, Feb. 2014, pp. 67-71.

[5]. Ms. Jasmin Bhambure, Ms. DhanashriChavan, Ms. Pallavi Band, Mrs.LakshmiMadhuri, “Secure Authentication Protocol in Client – Server Application using Visual Cryptography”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, February 2014, pp. 556-560.

[6]. Mohan V. Pawar, Anuradha J, “Security of network and Types of Attacks in Network”, International Conference on Intelligent Computing, Communication & Convergence, 2015, pp. 503 – 506.

[7]. MANJIRI N. MULEY, “ANALYSIS FOR EXPLORING THE SCOPE OF NETWORK SECURITY TECHNIQUES IN DIFFERENT ERA: A STUDY”, International Journal of Advanced Computational Engineering and Networking, Volume-3, Issue-12, Dec.-2015, pp. 33-36.

[8]. Rupam, AtulVerma, Ankita Singh, “An Approach to Detect Packets Using Packet Sniffing, International Journal of Computer Science & Engineering Survey (IJCSES) ,Vol.4, No.3, June 2013, pp.21-33.

[9]. Sharmin Rashid, SubhraProsun Paul, “Proposed Methods of IP Spoofing Detection & Prevention, International”, Journal of Science & Research (IJSR), Volume 2, Issue 8, August 2013, pp.438-444.

[10]. MukeshBarapatre, Prof. Vikrant Chole, Prof. L. Patil, “A Review on Spoofing Attack Detection in Wireless Adhoc Network”, International Journal of Emerging Trends & Technology in Computer Science, Volume 2, Issue 6, November – December 2013, pp.192-195.

[11]. Amandeep Kaur, Dr. Amardeep Singh, "A Review on Security Attacks in Mobile Ad-hoc Networks", International Journal of Science & Research, Volume 3 Issue 5, May 2014, pp.1295-1299.
[12]. Md. Waliullah, Diane Gan, "Wireless LAN Security Threats & Vulnerabilities", International Journal of Advanced Computer Science & Applications, Vol. 5, No. 1, 2014, pp.176-183.
[13]. P. Kiruthika Devi, Dr. R. Manavalan "Spoofing attack detection & localization in wireless sensor network", International Journal of Computer Science & Engineering Technology, Vol. 5, No. 09, Sep 2014, pp.877-886.
[14]. BarleenShinh, Manwinder Singh, "A Review Paper on Collaborative Black Hole Attack in MANET", International Journal of Engineering & Computer Science, Volume 3, Issue 12, December 2014, pp. 9547-9551.
[15]. Ms. VidyaVijayan, Ms. Josna P Joy, Mrs. Suchithra M S, "A Review on Password Cracking Strategies", international Journal of Research in Computer & Communication Technology, 2014, pp.8-15.